Fermilab GCSC Role and Responsibilities

Fermilab General Computer Security Coordinators (GCSC) serve an important role at Fermilab. They help communicate computing policies and enforcement actions to their respective Division, Section or Experiment. GCSCs are expected to communicate with their Division Head, Section Head, Spokespersons, administrators and their end user community. While line management is responsible for the acknowledgement and enforcement of computer security policies within their administrative domains, they may delegate some of the communication and awareness aspects to their appointed GCSCs, but such delegation is not to replace line management's involvement. GCSCs are expected to assist or delegate certain responsibilities in active or potential computer security incidents in the discovery, containment and cleanup phases. GCSCs are also tasked with reporting violations of computer security policies or potential incidents, and request exemptions to computer security policies or procedures.

GCSCs are appointed by their Division Head, Section Head or Spokesperson. Any large experiment may request GCSC representation, providing they first speak with their Division or Section GCSC to ensure duties will not conflict. In addition to the GCSC, a Deputy GCSC may also be appointed to lessen the burden of GCSC responsibilities and coverage. It is desired to acknowledge the GCSC role among the appointees' Performance Appraisal Goals. GCSCs are to attend GCSC meetings hosted by the Fermilab Computer Security Coordinator (FCSC). Typically, these meetings are scheduled once a month. GCSCs are also encouraged to participate in regularly scheduled System Administrator Round Table meetings. GCSCs may also be interested in attending the Unix Users and PC Manager meetings, held monthly, to discuss computer security and system administration practices.

GCSCs are active participants on the Fermilab Computer Security mailing list. This mailing list is the primary communication channel for non-critical computer incident reports and discussions. The content of these discussions are FNAL confidential material to be discussed only with the other members of the list or as needed in your role investigating an incident.

In addition to the Fermilab Computer Security list, each GCSC has control over a GCSC mailing list for their Division, Section or Experiment. The GCSC may add senior administrators or other responsible persons to this list to receive alerts pertaining to computer security incidents, policy violations or directed notices which affect their Division, Section or Experiment.

As the threat landscape changes, additional responsibilities may be asked of GCSCs. Additional responsibilities will be communicated in the GCSC meetings, Directorate Scheduling meetings and GCSC mailing lists. Every two years, this Role and Responsibilities document will be updated and distributed to reflect the new responsibilities.

Fermilab GCSC Role and Responsibilities (cont)

FNAL Security Coordination duties:

- Communicate awareness of computing risks to users and management. This awareness is to facilitate access to policies and procedures provided by the CSExec, FCSC, Fermilab Computer Security Team, FCIRT and supplemented by the Division/Section/Experiment specific plans, policies and procedures.
- Ensure alerts pertaining to both actual and possible computer security incidents (both automated and user initiated) within their Division/Section/Experiment are responded to. These responses may come directly from the associated GCSC or delegated to the local administrator(s) or end user. Automated email message alerts sent which require attention include (but are not limited to) automated email messages noting violations of the FNAL Computing Policies, missing critical patch notifications and alerts of outbound host or port scanning.
- Communicate the computer security incident reporting procedures through the appropriate defined channels and to provide updates of incidents occurring within their Division/Section/Experiment to their Division or Section Head or Spokesperson.
- Submit requests for Policy exemptions as defined by the Policy Exemption process for the affected policy
- Submit requests for Service exemptions as defined by the Service Exemption process for the affected service
- Communicate Critical Patch mandates and report any exceptions in their Division/Section/Experiment that cannot meet the terms of the mandate along with the reasons and remediation plans
- Acknowledge submitted Risk Assessments
- Submit Effort Reporting for both GCSC tasks for the month and System Administration efforts to attend to critical patching and policy violation efforts (when the effort reporting system is available)

FCIRT related duties:

- Assist FCIRT (Fermilab Computer Incident Response Team) in locating both the responsible persons and equipment involved in a computer security incident.
- Carry out triage and forensics (with approval from Division/Section Head or Spokesperson) as delegated by the FCIRT Head or FCIRT member coordinating the computer security incident.
- Assess potential risks of their Division, Section or Experiment during any given computer security incident.
- Assist in the communication of violations to computer security policy to line management, Division or Section Heads and Spokespersons where applicable.

Please sign below to indicate you have read and understand the responsibilities defined for the role of Fermilab GCSC and return it to Fermilab CD/Computer Security MS368.

_____	_____	_____
Fermilab ID	GCSC (or deputy) Signature	Date
_____	_____	_____
Fermilab ID	Division/Section/Spokesperson Signature	Date

Division/Section Name: _____